NOT FOR PUBLICATION UNTIL RELEASED BY
HOUSE COMMITTEE ON ENERGY AND COMMERCE
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS
UNITED STATES HOUSE OF REPRESENTATIVES

PRESENTATION TO THE
HOUSE COMMITTEE ON ENERGY AND COMMERCE
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS
U.S. HOUSE OF REPRESENTATIVES

SUBJECT: DOE Management and Oversight of Its Nuclear Weapons Complex: Lessons of the Y-12 Security Failure

STATEMENT OF: Brigadier General Sandra E. Finan
Commander, Air Force Nuclear Weapons Center
Based on Previous Position as
Acting Chief of Defense Nuclear Security, NNSA

March 13, 2013

NOT FOR PUBLICATION UNTIL RELEASED BY
HOUSE COMMITTEE ON ENERGY AND COMMERCE
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS
UNITED STATES HOUSE OF REPRESENTATIVES

Introduction

Chairman Murphy, Ranking Member Degette, distinguished Members of the Committee, thank you for the opportunity to discuss the study I conducted on the National Nuclear Security Administration's (NNSA) federal security organization and assessment model. Although I am no longer assigned to the NNSA, I am pleased to share our observations based on our 90 day study.

In the aftermath of the July 28, 2012 security incident at the National Nuclear Security Administration's Y-12 National Security Complex, the leadership of the NNSA and the Department of Energy (DOE) took action to address the security failures at Y-12. The initial information gathered revealed that issues at Y-12 were part of a larger pattern of security program management deficiencies within the NNSA. These security issues prompted the NNSA Administrator to commission a Task Force to analyze the current Federal NNSA security organizational structure and security oversight model and recommend possible improvements. The NNSA Administrator directed the Task Force to:

- Analyze current NNSA security organizational structure and recommend possible improvements that would improve operational focus, oversight, and culture sustainment.
- Analyze current NNSA security oversight model and mechanisms to determine what seams exist and what structures could be implemented to better ensure that the issues are found and fixed before they become problems.

While other reviews were aimed at diagnosing the root causes of the Y-12 event, the NNSA Administrator's direction called for this Task Force to focus on the "path forward" within the Federal NNSA organization. Under my leadership, the Task Force consisting of NNSA, DOE,

and military specialists conducted extensive document reviews and interviewed Federal managers and staff as well as a selection of contractor security managers and others across the NNSA security organization. The Task Force collected and analyzed information, identified issues, and suggested a revised organizational structure and assessment model.

While we highlighted negative aspects of the NNSA security organization and assessment model, the Task Force found many great people on the NNSA security staffs. They are clearly dedicated, skilled, and hard-working and want to get the security mission done right. Unfortunately, NNSA security personnel have seen themselves thwarted by lack of management support and feel obstructed by some of their peers. Their difficulties were compounded by the absence of a workforce strategy to recruit, retain, and develop a cadre of talented, knowledgeable and experienced security professionals. Thus, it is all the more encouraging that these personnel, almost without exception, genuinely care about doing good work. Their continued strong desire to build a successful security organization is a hopeful sign for the future.

Summary Findings

The Task Force noted significant deficiencies in security organization, oversight, and culture sustainment throughout the NNSA security organizations. In the NNSA security organizations, line management authority was ill-defined and claimed by multiple Federal NNSA organizations. On the one hand, the "Federal field organizations" (federal site offices and the nuclear production office which oversees the management and operating contracts) exercised line management authority over the site security contractors via the contract management structure. On the other hand, the NNSA Headquarters security organization asserted that it also had such authority. Absent clearly defined lines of authority, many individuals asserted authority, while correspondingly few have assigned responsibility. This lack of clear lines of authority

contributed to a widespread practice of decision-making by consensus. When consensus failed, organizational elements acted independently or not at all, which undermined effective implementation of the security program.

The Task Force further noted a significant gap in the current NNSA security organizational structure. At the strategic level the NNSA Headquarters organization had been ineffective and had intervened in field tactical execution. The Federal field organizations had been ineffective in performing their tactical responsibilities for executing the security program and had intervened in strategic matters. Additionally, there had not been a clearly identified operationally-focused organization that bridged the gap between strategic and tactical responsibilities and addressed standardization, field execution, and multi-site analysis.

The Task Force found a weak security performance assessment model. It found that NNSA relied overwhelmingly upon Federal staff simply reviewing contractor-provided data, rather than effectively assessing performance itself. At the same time, misinterpretation of the DOE Safety and Security Reform Plan resulted in less stringent independent oversight of security operations. As a result of numerous interviews, the Task Force also observed that potentially critical management information was not being reported clearly to the appropriate decision makers.

As concerning as these structural and assessment issues might be, the most striking result of this review falls in the area of culture sustainment. It quickly became evident that the Task Force findings closely resembled those presented in numerous prior reports. While NNSA has attempted to correct some identified issues over the years, it has not adequately emphasized effective security mission performance. In recent years, NNSA security leaders have chosen to emphasize security cost containment to the detriment of security program execution. The idea that the requirements for security performance effectiveness are subordinated to cost concerns

had become a prevailing concept in the NNSA security community. This emphasis had become endemic throughout the NNSA security culture, so much so that fundamental facility protection issues such as the protection of operational capabilities came to be regarded as too expensive and therefore "out of bounds" for analysis. The NNSA security culture had focused on fiscal limitations over effective performance. This resulted in an environment in which deficiencies were worked at the margins rather than management addressing core issues.

These issues underscored the critical role of effective leaders. While outside the charter of this Task Force, it must be acknowledged that leadership plays the key role in mission accomplishment. The Task Force recognized that effective leadership may compensate for structural deficiencies within an organization; however, restructuring alone cannot overcome leadership shortcomings. The best assessment model is useless if leaders fail to effectively implement it. Additionally, the assessment model will not be effective unless leaders consistently demand comprehensive, unbiased information. NNSA must take ownership of its history of security failures. Leadership must take bold and enduring actions if this pattern is to be broken.

NNSA Organizational Model

The existing NNSA security organizational structure was convoluted and ineffective. The Task Force observed that lines of authority in virtually every organizational function were divided. The NNSA security function was not well organized or effectively staffed and the NA-70 policy development and implementation process was sub-standard. While the Chief of Defense Nuclear Security is the Cognizant Security Authority (CSA), this responsibility has been unevenly delegated and was open to inconsistent interpretation. Security staffs were responsible to multiple lines of authority and for some functions may not be responsible to anyone. The most

fundamental issues arose from the relationship between NA-70 and the Federal field organizations. NA-70 believed that it had line management authority over the security elements within the Federal field organizations. However, the managers of these field organizations had been formally assigned line management authority. The NNSA Act states that the Chief of Defense Nuclear Security role includes "the development and implementation of security programs". The current interpretation of this provision has been a source of ambiguity due to the mixing of line and staff responsibilities.

Roles and responsibilities were either undefined or not followed. The Task Force identified numerous occasions across the NNSA security organizations where individuals were not allowed to perform assigned duties or assumed roles and responsibilities nominally assigned to others. The confusion of roles and responsibilities was evident in NA-70, within field organizations, and between NA-70 and the field. For example, the approved mission and function statements for the two major divisions within NA-70 have little apparent relationship to the way these offices operated and how they interacted with each other or with the NA-70. Within field organizations, the Task Force noted a number of instances where management precluded staff from performing the assigned roles of their position and/or assigned personnel to unrelated duties. At times, NA-70 acted as a formal line management organization, and asserted responsibilities that were formally assigned to the Federal field security organizations. NA-70 personnel were frequently frustrated by site-level resistance to the programmatic direction they provided and Federal field security managers were often similarly frustrated when NA-70 used its budget authority, its control over the policy process, and other activities to inject itself into what the sites regard as their line management decision-making process.

There were no clear lines of authority. There were overlapping lines of authority and mixed staff and line functions. The CSA function flowed from the NNSA Administrator through the Chief of Defense Nuclear Security to the Federal field organizations. Line management authority went from the NNSA Administrator through the Associate Administrator for Infrastructure and Operations (NA- 00), to the field. However, NA-70 attempted to exert line management authority and provided programmatic guidance directly to the Federal field security managers. While Federal field organizations administer the contracts governing the actual performance of the security mission, NA-70 routinely interacted with the security contractors. Furthermore, NA-70, not the line managers, was the primary executer of the NNSA security budget.

The security policy process was sub-standard. The Task Force identified that there was no clearly articulated or consistently implemented NNSA security policy process. A major concern was the supplanting of DOE Security Orders with generic and less restrictive NNSA policies (NAPs). This appeared to be based on a desire to reduce funding demands through a reduction of requirements. Additionally, the Task Force noted a desire on the part of some NA-70 senior managers to maximize separation from DOE HSS policies and activities. Within NA-70, policy and guidance were issued through a variety of formal and informal mechanisms with erratic distribution. The Task Force identified that some Federal field organizations were inconsistent in their acceptance and application of NA-70 issued policies. Finally, NA-70 policy and guidance tended to be vague resulting in widely differing interpretations by field personnel.

The NNSA Federal security organization was not effectively structured or staffed. While there were clearly strategic (Headquarters) and tactical (Federal field organizations and contractors) levels, there was little indication of an effective operational element with

responsibility for security program functions such as site assistance and standardization of program execution. The Task Force also noted that the Federal field organizations structured their security functions substantially differently. This resulted in a lack of standardization of both organization and execution of the security program. At some sites there was weakening of the security function and reduced senior management attention. There were a number of personnel issues associated with the security professional staff including the lack of a human capital development plan, no career path, and limited mobility. Additionally, the Task Force noted an overreliance on support service contractors who primarily assisted the NA-70 organization.

Federal Assessment Model

The Task Force expended considerable effort attempting to describe, understand and analyze the current assessment model and mechanisms.

The failure to adequately assess security system performance and to clearly and unequivocally report deficiencies to the appropriate senior managers has been identified as a significant contributing cause to the Y-12 security incident. The Task Force focused upon the performance assessment process as implemented by Federal field and Headquarters organizations within NNSA. Although contractor self-assessments were the first-line elements in the security performance assessment process, these were outside the direct scope of the review. Strengthening the contractor self-assessment process is an important objective, but cannot replace a rigorous Federal assessment process.

NNSA did not have an adequate security performance assessment process or capability. The performance assessment capabilities of Federal security organizations within NNSA were

virtually non-existent. Essentially all responsibility for performance assessment was delegated to the Federal field organizations. The current Federal field organizations were typically limited to "shadowing" contractor self-assessments and/or reviewing the reports these self-assessments generated. Moreover, there was a tendency on the part of some field Federal staff to adopt the role of defending "their" contractors rather than attempting to objectively assess contractor performance. At the Headquarters level, the NA-70 performance assessment function had only three full-time Federal staff members. The Task Force noted that the NA-70 assessment process was largely confined to the review of submitted paperwork. The result was that there was no NNSA Federal organization capable of performing effective security performance assessment.

The "systems-based" assessment model as implemented was ineffective for security. Misinterpretation, and/or misapplication of the DOE Safety and Security Reform Plan, dated March 16, 2010, resulted in a weakened Federal security assessment program. In particular, this document stated: "Security Performance: Contractors are provided the flexibility to tailor and implement security programs in light of their situation and to develop corresponding risk- and performance-based protection strategies without excessive Federal oversight or overly-prescriptive Departmental requirements." This guidance was further expanded upon and eventually articulated in NAP-21, Transformation Governance and Oversight Initiative. The belief arose that 'eyes on, hands off' precluded Federal security staff from conducting performance-based assessments of contractors. As a result, most Federal assessment was based on paperwork generated by the contractor. This paper-based system of assessment, without sufficient performance verification, was inadequate for effective evaluation of security operations.

NNSA had no clear and consistent performance baseline for security program implementation. A performance baseline, set forth in detailed standards and criteria, is the keystone of an effective security program. Precisely articulated standards and criteria further provide an objective foundation for performance assessment. NNSA did not have the standards or criteria necessary to effectively measure security program performance. The absence of such standards and criteria diminished the ability to identify potentially significant performance deficiencies. The Task Force noted that the lack of standards and criteria had been coupled with the widespread notion that contractors must only be told "what" the mission is, not "how" the mission is to be accomplished. While this approach may be appropriate in other areas, it was ineffective as applied to security programs. Therefore, security tasks were not necessarily performed in a manner consistent with NNSA security requirements.

The current assessment process was biased against criticism. The Task Force noted a distinct bias against finding and stating performance criticisms. The NNSA Federal assessment relies heavily on contractor self-assessment. While an important and useful tool, contractor self-assessments tend to be insufficiently objective. The primary Federal assessment role was performed by field staff. Long-term geographic proximity to site contractors can compromise the objectivity of these Federal assessors. Moreover, the intermingling of management and assessment roles within Federal field organizations can also contribute to less objective assessment. The NA-70 Headquarters performance assessment process, being paper-based, could not validate the information submitted. Information provided to the Task Force suggested that in some instances information considered to be unfavorable was being "watered down" or obscured. Furthermore, information was presented that indicate differing opinions were being

suppressed by some senior managers in the field and at Headquarters. As a result, NNSA senior leadership may not have received all information needed to make quality decisions.

Recommended Organizational Structure

Recommend an organizational structure that separates the line function for executing the security mission from the Headquarters staff function. Additionally, create an operational-level organization that focuses on security implementation and standardization. Distinct roles and responsibilities should be associated with tactical, operational, and strategic-level security functions. Tactical execution of contract administration occurs at the Federal field organizations. Operational implementation and standardization of operations across the security program occurs at the NA-00 level. Strategic-level policy guidance, requirements determination, and performance assessment occur in Headquarters NNSA, NA-70.

In order to clarify the line of authority, CSA must flow from the NNSA Administrator, through the head of the NA-00, to the Federal field managers, and finally to the designated CSA at field sites, with no re-delegations authorized to non-Federal individuals. This authority should follow the same path as the line authority. The asserted security line management tie between the Chief of Defense Nuclear Security and the security managers in the field should be terminated in order to ensure a single, clear line of authority.

In terms of clarifying line and staff functions, the current NA-70 organization needs to be restructured so that it serves solely as a staff organization at the strategic level. Specific alignment within the divisions can be varied. The most important change in NA-70 is the stand-up of the Performance Assessment Division -- a new function responsible for assessment of

contractor and Federal field organization performance. This is the entity that the Chief of Defense Nuclear Security would use to verify that security programs are properly implemented.

A new security operations organizational level needs to be stood up within the NA-00 structure. The responsibilities of this office are to ensure that the policies and guidance provided by the NA-70 staff are executed in the field. It will also ensure standardization of security procedures across the field locations as well as provide field assistance, and a conduit for field concerns to be surfaced to the NA-70 staff.

Resource planning and budgeting, and project management responsibilities will be realigned from NA-70 to the new operational-level organization. This establishes a clear linkage between budget formulation and mission execution and establishes an equally clear boundary between budget considerations and the formulation of requirements. An expanded intelligence/counterintelligence liaison is intended to ensure that Federal security managers get needed information and have appropriate ties to law enforcement and intelligence-related agencies.

At the tactical level in the field, the multiple lines of authority are eliminated and direction will come from a single line of authority. All authorities will run through the Federal field organization manager to the appropriate security manager. The Federal field organization scope of duties will include primary contract administrative functions--including reviews of contractor reports, analysis, security plans, and other required documentation; partnering with the executing contractor; remaining knowledgeable and up-to-date on the content, operations, and effectiveness of the contractor's security implementation; alerting management of all concerns related to contractor execution of the security mission.

This organizational structure will help define and clarify roles and responsibilities and facilitate a strong mission focus. It divides resourcing from requirements determination in order to ensure that requirements are appropriately stated, weighed against budget resources and decisions made on accepting risks at the appropriate level. It provides a single line of authority to those operating in the field and maintains an appropriate span of control.

Recommended Assessment Model

Recommend a three-tiered assessment process that strengthens the role of Federal security assessment within NNSA without diminishing the legitimate need for contractors to maintain their own self-assessment capabilities.

The contractor self-assessment process continues as a first tier in the overall assessment process. The primary audience for the contractor self-assessments should be the contractor security managers themselves. However, the self-assessments should follow a consistent, program-wide format, and be made available for review at all higher levels of management. Contractors should be required to identify, report, and resolve security issues--sanctions should come when a higher level assessment uncovers problems that the contractor self-assessments fail to identify or properly address. Even when an issue is readily resolved and corrective actions are immediate, a finding should be issued and the corrective action recorded. Failure to do so inevitably hides potential negative trends. Contractor self-assessments should involve active performance testing rather than simply relying on work observation and document review--effective security performance can only be evaluated through testing.

The fundamental purpose of Federal security performance assessment is to ensure that requirements are properly implemented. Therefore, the primary Federal assessment organization

should ultimately report to the Chief of Defense Nuclear Security, who is responsible for requirements. This provides independence not only from the contractors, but also from the tactical-level Federal field staff whose necessary day-to-day interaction with contractor managers and staff risks loss of objectivity. This enables the Chief of Defense Nuclear Security to better ensure effective implementation of NNSA security programs. Additionally, it provides feedback on performance to the operational and tactical levels.

These Federal security assessments should include performance testing of all critical elements. The assessors should issue clear findings which are to be tracked and closed in a program-wide corrective action management system. Federal assessors should also look closely at the contractor self-assessment process; "failures to identify" by the contractor self-assessment element should automatically rise to the level of significant findings.

The final tier of the assessment model should explicitly rely upon the services of the independent security oversight function currently provided by HSS. NNSA should arrange for a regular process of comprehensive inspections. The oversight function should be encouraged to issue strong findings for matters of potential concern to the NNSA Administrator and the Secretary of Energy, and should routinely evaluate the performance of contractor self-assessments and the Federal assessment program.

This performance assessment model assumes a common requirements base that is employed at all levels and across the NNSA security program. While some allowance may be made for site-specific issues, the fundamental elements of this requirements base should be an appropriately integrated system of DOE policies, NNSA implementation directives, and field operational guidance. The requirements base should be reflected in approved documents such as site Safeguards and Security Plans. Specific performance requirements should be articulated in

detailed performance standards and criteria supported by a commonly understood and utilized performance testing process.

Closing

Over the years, there has been tension between implementation of security and conduct of operations. Whenever there have been significant incidents of security concern, there have been corresponding swings of the pendulum towards a more rigorous security program. Security program emphasis has increased after espionage cases, internal security lapses, and external events such as the September 11, 2001 attacks. However, over time, the general trend has been to accept more risk and to reduce the perceived burden and cost of the security mission. Furthermore, the trend has been to remove security from an integral mission role, adversely affecting the NNSA security program. The events at Y-12 illustrate how far the pendulum has swung in the wrong direction.

The Secretary of Energy characterized the Y-12 events as "unacceptable" and clearly stated that security is the highest organizational priority. The NNSA Administrator has been equally emphatic in numerous public statements since the incident. The evidence from Y-12 and from prior security incidents points to a culture of compromises. Moving forward, NNSA must establish and sustain an effective security program. NNSA must address the significant flaws in the current organizational structure for security and the associated assessment model. NNSA must clearly and consistently emphasize the importance of security. Ensuring that the right leadership is in the right position is absolutely critical to success. The daunting prospect—and the one that will require the consistent emphasis of current and future Secretaries of Energy and future Administrators of the NNSA—will be to instill a culture that embraces security as a

fundamental and essential element of the NNSA mission. If NNSA fails in this, then senior leaders will again find themselves answering to the American people for the failures of security. Sooner or later, the perpetrator will not be peacefully-minded.